WORKPLACE PRIVACY & PRIVATE SECTOR PRIVACY LAWS

David Loukidelis
Information and Privacy Commissioner for British Columbia

CLE Employment Law Conference
Vancouver BC

April 24 & 25, 2003

I. Introduction

There are many arbitration and court decisions dealing with workplace privacy issues. These decisions have struggled, particularly in recent years, to strike a balance between employee privacy and employers' ability to protect their business interests. Other trends in employment-related privacy are, however, discernible.

Over the past 30 years, legislatures around Europe have legislated to protect privacy in both the public and private sectors. Until recently, Canadian legislators had focussed on privacy protection only in the public sector. This is no longer true. Canada has been catching up with Europe – and the United States – over the last decade. Quebec was first off the mark, extending its existing privacy law to the private sector in 1994. More recently, and critically for the purposes of this paper, Parliament in 2000 enacted the *Personal Information Protection and Electronic Documents Act* ("PIPEDA")[1]. PIPEDA came into force on January 1, 2001 in the federally-regulated sphere. Alberta is slated to table its private sector privacy law this month. Ontario last year undertook extensive consultations on a draft private sector privacy law and has a Bill ready to go. It was put on the back burner last December, however, apparently until after the Ontario election later this year.

In British Columbia, the provincial government has repeatedly affirmed its intention to introduce legislation governing private sector privacy practices. The legislation, expected this spring, would implement the unanimous recommendation, in 2001, of the Special Committee on Information Privacy in the Private Sector, an all-party committee of the Legislative Assembly, that such legislation should be enacted.

This paper is limited to a general examination of the nature and implications of private sector privacy legislation. It paper does not address privacy issues reflected in arbitration and court decisions. Papers delivered at CLE courses in recent years have done an excellent job of surveying the case law and can be expected to do so again in future years.[2]

---

[1] S.C. 2000, c. 5. A copy is at: http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html.

[2] See, for example, Bill Trott & Mark Grady, 'Privacy and Labour Arbitration' (Labour Arbitration CLE, June 2002); and Gary T. Clarke, 'Technology and Privacy Issues' (CLE Employment Law Conference, April 2002).

This paper begins with a general overview of the international context for private sector privacy laws, their history in Canada and the principles that generally underpin such laws. This overview is necessary to understand why Canadian law is developing as it is.

Because a British Columbia law had not been tabled at the time of writing, one can only speculate on how a British Columbia law would affect workplace privacy. That speculation is driven by PIPEDA, since a British Columbia law must, as discussed below, be substantially similar to PIPEDA to preclude its application in British Columbia.

II. Context For Canada's Private Sector Privacy Laws

1. International Developments

The 1948 United Nations *International Declaration of Human Rights* explicitly acknowledged the right to privacy, but statutory responses to privacy concerns, driven in part by fears associated with increased computerization of personal information, were slow in coming. The international trend toward privacy protection in the public and private sectors really only got under way in earnest in the 1970s.

In 1973, Sweden enacted its *Data Protection Act* and, in 1977, Germany enacted data protection legislation.[3] Similar statutes were enacted in 1978 in France, Denmark and Norway. All of these laws cover both the public and private sectors. In the United States, Congress in 1978 enacted the federal *Privacy Act*, which governs federal government institutions, but comprehensive private sector legislation was not forthcoming at that time and has yet to be enacted. It is sometimes thought that the U.S. does not protect privacy in the private sector. This is not correct. Many state and federal laws regulate private sector privacy practices, although they tend to be issue-specific and arguably piecemeal.[4]

There have long been concerns about privacy laws creating obstacles to trade. In 1980, the OECD adopted *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, to which Canada became a signatory. The OECD Guidelines acknowledge that, as flows of personal information across national borders increase through the globalization of

---

[3] European countries refer to 'data protection', as opposed to 'privacy protection'. Observers love to argue about whether 'data protection' differs from 'privacy protection', but for present purposes the terminology is interchangeable.

[4] Financial privacy is protected, for example, under the Gramm-Leach-Bliley Act of 1998. Other U.S. federal laws protecting privacy *include* the *Children's Online Privacy Protection Act* (1998), the *Health Insurance Portability and Accountability Act* (1996), the *Driver's Privacy Protection Act* (1994) and the *Electronic Communications Privacy Act* (1986). In addition, in 2000 the U.S. and the European Union agreed on the Safe Harbour compromise. This allows any U.S. company to voluntarily abide by the European Union Directive on personal information, discussed later in this paper, under penalty of sanction by the Federal Trade Commission for deceptive trade practices where the company has not complied with its privacy obligations. Companies in the Safe Harbour include Microsoft, IBM and Hewlett Packard. Within the last year there have been hints that the FTC is coming around to the view that a comprehensive statutory approach is needed. On March 31, 2003, Sen. Diane Feinstein (D., Cal.) introduced the 'Privacy Act of 2003' (S.745), which would regulate private sector privacy practices federally. Her Bill received two readings and was referred to the Senate Committee on the Judiciary on March 31. See http://thomas.loc.gov/cgi-bin/bdquery/z?d108:S00745:@@@L.

commerce, national laws might inhibit the exchange of personal information for commercial purposes. The OECD Guidelines are intended to guide member states in the development of harmonized domestic legislation, with a view to minimizing trade disruptions. The OECD Guidelines acknowledge what are now commonly known as 'fair information practices'. The number and definition of the various fair information practices vary in different formulations, but the OECD version is very close to the ten principles that ultimately became enshrined in PIPEDA. The OECD Guidelines are voluntary, as is the 1985 OECD *Declaration on Transborder Data Flows*, which Canada also signed. But both documents say that member states should enact harmonized privacy regulations.

In Europe, the European Union in 1995 moved ahead with regulations, consistent with the OECD Guidelines, by enacting a Directive, sometimes referred to as the *Directive on the Protection of Personal Data and on the Free Movement of Such Data.*[5] EU members were given until October of 1998 to achieve the intended objective of harmonization of privacy laws across Europe. The EU Directive also contemplates a ban on the export from the EU of any personal information to any state that does not offer an adequate level of protection for personal information, as determined by the EU.[6]

2. Canadian Developments

(a) Quebec

Quebec has had a private sector privacy law since 1994,[7] anticipating both the EU Directive and PIPEDA. There have been no horror stories, by any stretch, in terms of the regulatory impact of the Quebec law.

(b) Federal *Personal Information Protection and Electronic Documents Act*

Soon after the EU Directive was enacted, a multi-year effort by a broad spectrum of Canadian businesses to fashion a voluntary private sector privacy code came to fruition in the form of the Canadian Standards Association's *Model Code for the Protection of Personal Information* ("CSA Code")[8]. In light of the EU Directive, however, the federal government realized that, to forestall possible trade problems with the EU, a legislative approach was needed. Parliament's response was PIPEDA, which came into force on January 1, 2001 in relation to federally-regulated businesses.

---

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data, Official Journal n° L 281 of 23.11.1995, p. 31, available at: http://europa.eu.int/comm/internal_market/en/dataprot/law/index.htm

[6] EU Directive, Art. 26

[7] *An Act Respecting the Protection of Personal Information in the Private Sector*, S.Q., c. P-39.1.

[8] CAN/CSA-Q830-96, a National Standard of Canada.

Section 26(2) of PIPEDA provides that the federal Cabinet may, by Order in Council,

> ... if satisfied that legislation of a province that is substantially similar to this Part applies to an organization, a class of organizations, an activity or a class of activities, exempt the organization, activity or class from the application of this Part in respect of the collection, use or disclosure of personal information that occurs within that province.

Failing such an exemption by the federal Cabinet, s. 30(2) removes, effective January 1, 2004, the present s. 30(1) exemption from PIPEDA for any organization that is not a federal work, undertaking or business. Put another way, PIPEDA purports to give the federal Cabinet the power to deem a province's private sector privacy law worthy of the name, failing which PIPEDA applies to commercial activities in the province.

Given this approach, PIPEDA is undoubtedly driving the development of private sector privacy laws in Canada. It is discussed below in some detail.

(c) Ontario

In Ontario, the provincial government in 2002 released a draft law called the 'Protection of Personal Information Act, 2002'. That draft elicited a good deal of debate and was revised pretty substantially, eventually achieving acceptance by pretty well all stakeholders. The Ontario government has not, however, proceeded with a Bill at this time, apparently because of the election expected later this year.

(d) British Columbia & Alberta

At the time of writing the British Columbia provincial government had not introduced a Bill to address private sector privacy, although one is widely expected during this sitting of the Legislative Assembly. In light of PIPEDA's role, it is safe to assume that any British Columbia law will be fashioned around the fair information practices articulated in the CSA Code and enshrined in PIPEDA. A safe, prediction is that British Columbia's law will look much like Alberta's private sector privacy statute, the tabling of which is expected this month[9].

---

[9] It is widely known that officials from British Columbia and Alberta have for several months been working together in an attempt to fashion private sector privacy laws for those provinces that are as close to being the same as is possible. If this works out, Alberta and British Columbia will enact harmonized legislation, which will ease the compliance burden in those provinces.

III. Discussion of PIPEDA

1. What Does PIPEDA Apply To?

(a) PIPEDA Applies to Personal Information

PIPEDA applies to the "personal information" practices of organizations. PIPEDA defines "personal information" as information "about an identifiable individual", but not "the name, title, or business address or telephone number of an employee of an organization." The federal Privacy Commissioner has ruled that "personal information" is not limited to *recorded* personal information, since the term "recorded" is not used in the statutory definition[10].

The definition of "personal information" refers to information "about" an identifiable individual. In a 2001 decision,[11] the federal Privacy Commissioner ruled that information about the prescribing patterns of physicians, which pharmacists were selling without consent, was not information "about" the physicians, but was work product information not protected by PIPEDA.[12] The Privacy Commissioner characterized the data as information relating to the "professional process that led to its issuance", *i.e.* the result of the "physician's work activity." By parity of reasoning, one could expect that an employee's work product, in the sense of information created through one's employment activities, would not be considered information "about" the individual employee within the meaning of PIPEDA. If information consists of, for example, a performance evaluation of an individual employee, the 'work product' concept will not apply. To the extent an assessment judges the employee's discharge of his or her employment duties or functions, it will be that employee's personal information for the purposes of PIPEDA.

---

[10] PIPED Act Case Summary #1 (June 15, 2001). These summaries are found at www.privcom.gc.ca.

[11] PIPED Act Case Summary #14 (October 2, 2001). A comment is necessary about PIPEDA case summaries. The summaries are generally very brief and only state findings and conclusions. The Privacy Commissioner's office has declined to disclose full sets of reasons, even though decisions can be written and published in anonymized fashion if privacy is the concern. The practice of publishing summaries makes it difficult to discern the reasoning and evidentiary findings that underpin decisions, even though certainty and predictability are important values for all stakeholders (notably affected businesses). The federal Privacy Commissioner's office has, it should be noted, produced a useful guide for businesses and other organizations called *Your Privacy Responsibilities*: www.privcom.gc.ca/information/guide_e.pdf

[12] This decision is under appeal to the Federal Court of Canada and, at the time of writing, no decision had been rendered. Though by no means determinative, it is interesting to note the tension between this 'work product' concept and the Supreme Court of Canada's views on what is personal information, under the federal *Privacy Act*, in *Canada (Information Commissioner)* v. *Commissioner of the RCMP*, 2003 SCC 8, and *Dagg* v. *Canada (Minister of Finance)*, [1997] 2 S.C.R. 403.

It is not clear, however, where the federal Privacy Commissioner will draw the line between so-called 'work product' information and personal information. He appears to have treated video surveillance of employees performing their work duties, for example, as a collection of "personal information" within the meaning of PIPEDA[13].

(b) PIPEDA Applies to Commercial Activities of Organizations

PIPEDA applies only to organizations. It defines an "organization" as including "an association, a partnership, a person and a trade union." This does not mean it applies to all private sector activities. It applies only in respect of personal information that an organization collects, uses or discloses "in the course of commercial activities" (s. 4(1)(a)) or that "is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business" (s. 4(1)(b)). The term "commercial activity" is defined as meaning any

> … particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

Much has been made of the vagueness of this definition, which does invite circularity. Businesses and their legal advisers may have to seek solace by resorting to income tax cases for guidance on what is a commercial activity.

Where no substantially similar provincial private sector privacy law operates, PIPEDA will apply only to commercial activities, not non-profit activities.

Further, it will apply to personal information of employees of a federal work, undertaking or business, but not other employees. Section 4(2)(b) provides that PIPEDA applies to personal information of employees of a federal work, undertaking or business (s. 4(2)(b)). The relationship between employer and employee is not considered to be of a commercial character; it falls within the provincial constitutional competence over property and civil rights. See, for example, *Toronto Electric Commissioners* v. *Snider*[14] and *Oil, Chemical and Atomic Workers International Union, Local 16-601* v. *Imperial Oil Limited et al.*[15] So while PIPEDA will apply to personal information of employees of a branch of a federally-chartered bank on one side of the street, the employees of a branch of a provincially-regulated credit union across the street will not be covered.

---

[13] PIPED Act Case Summary #114 (January 23, 2003).

[14] [1925] A.C. 396 (P.C.)

[15] [1963] S.C.R. 584.

2. Main Features of PIPEDA

PIPEDA reflects a curious approach to statutory drafting. Apparently in an effort to meet possible business community concerns about legislating privacy protection, as opposed to leaving EU Directive compliance to the voluntary CSA Code, the federal government more or less stapled the CSA Code to the back of a bare-bones Bill. Although Part 1 of PIPEDA contains substantive provisions, they supplement the CSA Code, which has been given statutory force. The difficulty, of course, is that the CSA Code was drafted as a *voluntary* code, which means a good deal of its language is imprecise. One therefore finds provisions such as s. 5(2) of PIPEDA, which says the word should, when used in the CSA Code, "indicates a recommendation and does not impose an obligation." This approach to statutory drafting will, one hopes, be avoided in British Columbia.

PIPEDA enshrines the fair information practices, or principles, found in the OECD Guidelines. The fair information practices reflected in the CSA Code can be summarized as follows:

- *Accountability* – An organization must designate someone to be internally responsible for compliance.
- *Identifying purposes* – An organization must identify the purposes for which personal information is collected at or before the time the information collected.
- *Consent* – The knowledge and consent of the individual are required for collection, use or disclosure of personal information (except where inappropriate).
- *Limiting collection* – An organization must limit its collection of personal information to that which is necessary for the purposes identified and must collect information only by fair and lawful means.
- *Limiting use, disclosure and retention* – An organization must not use or disclose personal information for purposes other than those for which it was collected, except with the individual's consent or as required by law. An organization must retain personal information only as long as is necessary for the fulfillment of the identified purposes.
- *Accuracy* – An organization must ensure that personal information is as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.
- *Safeguards* – An organization must protect personal information by security safeguards appropriate to the sensitivity of the information.
- *Openness* – An organization must make readily available to individuals specific information about its policies and practices relating to the management of personal information.
- *Individual access* – An organization must inform individuals of the existence, use and disclosure of their personal information and must give individuals access to their personal information. This must include the ability to challenge the accuracy and completeness of the information and have it corrected as appropriate.
- *Challenging compliance* – An organization must afford individuals mechanisms for challenging compliance with the principles.

The following discussion deals with how PIPEDA fleshes out these principles.

3. Specific PIPEDA Requirements

PIPEDA imposes certain obligations on organizations respecting their collection, use, disclosure, retention and safeguarding of personal information. The following discussion focusses, of course, on employee personal information.

(a) Limits on Collection of Personal Information

Section 5(3) of PIPEDA limits an organization's ability to collect, use and disclose personal information:

> An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

Further, clause 4.4 of the CSA Code stipulates that collection of personal information must be limited to "that which is necessary for the purposes identified by the organization."

The federal Privacy Commissioner has on several occasions considered whether an organization was authorized to collect personal information in light of s. 5(3). He has also considered whether personal information an organization had collected was "necessary" for the stated purposes or went beyond it. He has, for example, indicated that s. 5(3) is relevant in determining whether collection of personal information through workplace video surveillance is permitted under PIPEDA[16]. In another case, he held that the information an employer required an employee to provide in claiming sick leave benefits did not go beyond what was "necessary" for the stated purposes and was thus permitted under s. 5(3) and clause 4.4[17].

(b) Consent Is Generally Needed for Collection, Use or Disclosure

Clause 4.3 of the CSA Code stipulates that the "knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate."

PIPEDA does not stipulate that consent must be explicit or written in all cases. This flows from clause 4.3 of the CSA Code. Clause 4.3.4 acknowledges that the "form of the consent sought by the organization may vary, depending on the circumstances and the type of information." It goes on to say that an organization must take into account the "sensitivity of the information" in deciding which form of consent to use. As an example, it suggests that

---

[16] See, for example, PIPED Act Case Summary #114 (January 23, 2003), in which the Privacy Commissioner relied on s. 5(3) to import a four-part test for whether workplace video surveillance is demonstrably justified and thus permitted under PIPEDA. Also see PIPED Act Case Summary #119 (February 17, 2003), where the employer's requirement that an employee submit medical information to support a request for transfer was held to be appropriate in light of, among other things, s. 5(3).

[17] See PIPED Act Case Summary #118 (February 17, 2003).

information such as medical information or income-related information "is almost always considered to be sensitive". Clause 4.3.6 of the CSA Code suggests that an organization should "generally seek express consent when the information is likely to be considered sensitive." The suggestion that express consent is, in the case of sensitive information, "generally" a good idea should not lull employers into complacency. Where sensitive personal information is involved, express, written consent is, out of an abundance of caution, better. In cases where less sensitive information is involved, an employer can rely on implied consent, which is acknowledged by clause 4.3.6 of the CSA Code as a legitimate form of consent where less sensitive information is involved.

Perhaps the clearest example of sensitive information that should only be collected with an employee's explicit written consent is health information. An employer seeking to collect health information about its employees without explicit written consent is, of course, unlikely to enjoy much success anyway. As a matter of good practice, however, employers should seek consent for collection of personal health information about employees. Nor is it desirable to try fashion broad consents, signed at the outside of the employment relationship, to cover future collection of sensitive personal information. It will be difficult to frame such a standing consent sufficiently specifically to cover all possible uses down the road. This risks rendering the consent useless altogether. Moreover, a policy of obtaining consent to collection, use and disclosure of sensitive information (including employee health information) only as and when actually needed is also preferable as a matter of good employee relations.

The need for explicit consent respecting sensitive personal information will not unduly hamper employers. The federal Privacy Commissioner has found that PIPEDA authorizes an employer to require an employee on extended sick leave to consent to disclosure by his physician of medical information related to the employee's illness.[18] That case involved a consent that the employer required for the specified purpose of administering the extended sick leave program and only sought once the employee had put his health an issue by claiming extended sick leave.

Another PIPEDA principle that affects the seeking or giving of consent is that, in certain circumstances, consent cannot be coerced. Clause 4.3.3 of the CSA Code prohibits organizations from requiring individuals to consent to the collection, use or disclosure of information "beyond that required to fulfill the explicitly specified and legitimate purposes." This limitation only applies, however, where an organization seeks to require consent "as a condition of the supply of a product or service". This limitation is not, on its face, likely to apply within the employment context.

---

[18] PIPED Act Case Summary #118 (February 17, 2003). The cases dealing with employee consent to collection of personal medical information for sick leave purposes also illustrate the need for employers to ensure that information so gathered is only disclosed and used within the employer's organization by those individuals who have a need to know that information and to use it for the stated purposes.

Having said this, clause 4.3 of the CSA Code and s. 5(3) of PIPEDA in combination limit an employer's ability to collect, use or disclose employee personal information. As mentioned earlier, s. 5(3) provides that an organization may only collect, use or disclose personal information for "purposes that a reasonable person would consider would consider are appropriate circumstances" and clause 4.4 limits collection of personal information to that which is "necessary for the purposes identified by the organization." As long as an employer proposes to collect, use or disclose employee personal information for purposes that a reasonable person would consider appropriate, and that collection is part of or becomes part of the terms employment, an employee may have little choice but to consent or face employment discipline or loss of employment.

In one PIPEDA case, a number of employees of the nuclear products division of a company alleged that their employer had inappropriately required them to consent to the collection of their personal information for the purposes of a security clearance check. [19] The employee's union had negotiated an agreement with the employer under which any employee who did not pass the security check would be able to transfer to another of the company's operations, although not necessarily at the same job level. Failure to consent could mean dismissal from employment. The employees argued that their consent to the collection was not voluntary given the negative consequences if they refused consent.

The federal Privacy Commissioner decided that a reasonable person would consider it appropriate in the circumstances for the employer to collect personal information for the purpose of conducting security clearances. He noted that the Canadian Nuclear Safety Commission had ordered its licensees, including the employer, to not permit any person to enter or remain in a licensed facility unless that person had a facility-access security clearance. The company risked losing its licence to produced nuclear fuels if it has refused to comply with security clearance requirement. This drove the employer to require criminal record checks or full background checks.

The Privacy Commissioner concluded it was "reasonable" for the employer to comply with a "reasonable order" and therefore to collect the personal information for the purpose of the security clearance checks. Although the Privacy Commissioner acknowledged that the complainants would have felt pressure to consent, given the possible negative consequences for their employment, their consent was nonetheless voluntary. He considered that the key consideration under PIPEDA was not whether there might be consequences if an individual refused to give consent, but rather whether the collection itself was reasonable in the circumstances.

---

[19] PIPED Act Case Summary #65 (August 14, 2002). It is not clear how the finding that the CNSC's order was "reasonable" entered the PIPEDA analysis. It may be the Privacy Commissioner considered it necessary, and within his authority, to inquire into the validity of the CNSC order. On the consent point, also see PIPED Act Case Summary #127 (March 4, 2003), where the federal Privacy Commissioner reiterated that, even where there are potentially negative consequences for refusing consent, an employee can be required to consent to collection of personal information for security clearance purposes. That case dealt with a telecommunications company's compliance with federal security clearance requirement for airports and airport facilities.

The last point about consent is that an organization must not obtain consent "through deception" (clause 4.3.5, CSA Code). It is not clear how much this adds to the separate requirements that organizations only collect, use or disclosure personal information for reasonable purposes, to the extent necessary for those purposes, and only using "fair and lawful means" (clause 4.4, CSA Code). A similar comment can be made about the clause 4.4 prohibition against collecting personal information other than through "fair and lawful means".

(c) Exceptions to Requirement of Consent for Collection

Section 7(1) of PIPEDA provides that, for the purposes of clause 4.3, an organization may *collect* personal information without an individual's knowledge or consent in certain circumstances. The circumstance most likely to be pertinent in the employment context is found in s. 7(1)(d), which allows collection without consent if

> … it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or contravention of the laws of Canada or a province.

An obvious example of where consent may be dispensed with is where an employer is investigating a suspected case of employee fraud. That investigation would qualify under s. 7(1)(d) as both an investigation into a contravention of the laws of Canada – the *Criminal Code of Canada* – and "breach of an agreement", *i.e.*, breach of the employee's implied (or express) contractual duty of honesty. This is sensible. One can hardly expect an employer to ask an employee for consent to investigate the employee's suspected criminal wrongdoing. The employer should be allowed to collect information that is necessary for the investigation, and disclose it only for law enforcement purposes, but not be forced to tip its hand by seeking consent.

Another possibly relevant exception to the requirement for consent to collection is found in s. 7(1)(a). One example of how this might come into play is where an employer wishes to use a head-hunter to identify prospective employees without their knowledge. Section 7(1)(a) might be stretched to allow such indirect, non-consensual collection of personal information on the basis it is "clearly in the interests of the individual and consent cannot be obtained in a timely way". It is doubtful whether this provision was actually intended to cover this situation, however, but it is really the only hole for the peg. One can only hope that the British Columbia legislation will offer more flexibility on this score.

(d) Exceptions to Requirement of Consent for Use

If an employer has collected employee personal information for one purpose, it cannot generally use it for other purposes without consent. The consent rule is, however, overridden in a number of circumstances. Section 7(2) of PIPEDA provides that an organization may *use* an employee's personal information without his or her knowledge or consent in a variety of circumstances. One that is likely to be applicable in the employment context is found in s. 7(2)(a), which allow use of employee personal information where,

> ... in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention.

Taking the above employee-fraud example, if an employer has collected the employee's personal information indirectly and has discovered evidence of fraud, it may turn the evidence over to the police. Section s. 7(2) authorizes that disclosure without consent.

Section 7(2)(b) also allows use of personal information without knowledge or consent if

> ... it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual.

(e) Exceptions to Requirement of Consent for Disclosure

Last, s. 7(3) authorizes an organization to *disclose* employee personal information without the knowledge or consent of the employee in certain circumstances, including disclosure:

- To a lawyer acting for the organization (s. 7(3)(a));
- For the purpose of collecting a debt owed by the individual to the organization (s. 7(3)(b));
- In order to comply with a subpoena, warrant or order compelling disclosure (s. 7(3)(c));
- To the appropriate federal government institution charged with the responsibility for money laundering investigations (s. 7(3)(c.2);
- Made to an investigative body or government institution where there are reasonable grounds to believe the information relates to a breach of an agreement or a law (s. 7(3)(d)); and
- When information is disclosed to someone who needs it because of an emergency that threatens the life, health or security of an individual (s. 7(3)(e)).

(f) Hiring Practices As An Example of PIPEDA's Impact

This discussion uses the hiring process as an example of some of the issues PIPEDA and similar laws will raise in the employment context.

Personal information is collected to hire employees. This information ranges from simple demographic information to information about education and work history. In many cases, job applicants fill in application forms to provide relevant particulars. Several points arise.

First, as contemplated by s. 5(3) of PIPEDA and clause 4.4 of the CSA Code, an employer must collect only the information that is necessary to hire someone and that a reasonable person would consider appropriate in the circumstances. For example, it would be the rarest of cases where an employer could legitimately claim that it needed information about a prospective employee's personal political beliefs in order to hire that individual. A more likely example (one would hope) is of an insurance company seeking to hire part-time clerical staff for its legal department. Questions as to the nature, timing and quantity of applicants' consumption of alcohol are wide of the mark, since such information is not reasonably necessary for the contemplated purposes. The rule-of-thumb for an employer should be whether personal information it proposes to collect is necessary and reasonable for the purpose of selecting qualified applicants for employment in the position.

The second point is that express consent should be obtained. Where an application form is used, employers should, instead of relying on implied consent, ensure the application form includes notice and consent. Here is an example of a possible notice and consent:

> We are collecting your personal information on this form to determine your suitability for the position you have applied for and, if we hire you, for the purpose of our employment relationship. We will use and disclose your personal information only for those purposes or as permitted or required by law. By signing this form, you consent to our collecting, using and disclosing your personal information for these purposes. If you have any questions about this, you can contact [*insert name of the position held by the responsible privacy contact*].

This notice refers, of course, to more than just the hiring process. It explicitly provides that the information collected on the form may be used for the purposes of the "employment relationship". This is intended to cover situations in which the employer might wish, for example, to discipline or dismiss an employee who, the employer later discovers, has provided false information in support of her or his job application. The notice also notifies the applicant that the employer may use or disclose the information as permitted or required by law, *e.g.*, where the employer discloses the information to its legal counsel to get advice about disciplining the employee (s. 7(3)(a)) or where required by court order (s. 7(3)(c)).

Under a PIPEDA-like law, where an employers asks applicants for references on the job application form itself, it would be a good idea to ensure that the consent covers such collection and use of personal information, perhaps using language such as this:

> You also consent to our getting information about you from any references you have specified in this application and to our using that information for the purposes just described.

In cases where the employer might also wish to 'ask around' about an applicant without being limited to specified references, this prospect could also be mentioned:

> You also consent to our inquiring about your suitability for the position by making inquiries of persons other than references you have specified in this application.

An example is given above of difficulties an employer might face under PIPEDA in using a head-hunting firm to identify possible job candidates without their knowledge. In some cases, the individual will have approached the headhunting firm and asked to have his or her name added to list of possible candidates. In such a case, the head-hunting firm should cover its bases by getting the individual's explicit consent to collection of her or his personal information, at that time by the head-hunting firm and later by indirect means if necessary. It should also get consent to disclosure of the information to prospective employers and to their use of that information. This should be done as part of the sign-up process.

4. Employees' Right of Access to their Own Personal Information

PIPEDA gives individuals, through clause 4.9, a right of access to their own personal information. Space does not permit a review here of the details of how that right can be exercised, or the various time limits that apply to it, but some outline of the exceptions to that right of access is desirable. It is reasonable to speculate that British Columbia's private sector privacy legislation will incorporate similar exceptions to the right of access, there being no doubt that the legislation will have to afford a right of access in order to be considered substantially similar by the federal Cabinet.

Section 9 of PIPEDA prohibits an organization from giving an individual access to "personal information if doing so would likely reveal personal information about a third party." As is the case under s. 4(2) of British Columbia's *Freedom of Information and Protection of Privacy Act*, the organization must sever third-party personal information before giving the individual access to his or her own personal information. Third-party personal information can be disclosed, however, if the third party consents to the disclosure or the individual needs the information because "an individual's life, health or security is threatened" (s. 9(2)).

In addition, s. 9(3) authorizes organizations to refuse access to personal information where:

- The information is protected by solicitor-client privilege (s. 9(3)(a));
- To do so would reveal confidential commercial information (s. 9(3)(b));
- To do so could reasonably be expected to threaten the life or security of another individual (s. 9(3)c));
- The information was collected as reasonable for purposes relating to investigating a breach of an agreement or contravention of the laws of Canada or province (s. 9(3)(c.1));
- The information was generated in the course of a formal dispute resolution process.

In such cases, consistent with the severing duty under s. 9(1), organizations must sever protected information and disclose the balance if the protected information "is severable from the record containing any other information for which access is requested".

A number of decisions under PIPEDA deal with these various exceptions. In one case, a railway company employee complained that he had been denied access to a portion of his personal information. The company had withheld a letter that it had sent to the employee's physician. The federal Privacy Commissioner ruled that the only third-party references in that letter were to the physician, to whom the letter was addressed, the company employee who wrote the letter, an unnamed company manager and the company's own physician. He held that the letter contained information about the employee and that, to the extent that third parties were mentioned, they were mentioned in a business capacity. Accordingly, the letter could not be withheld.[20].

The preceding case also illustrates the application of s. 9(3)(c), since the railway purported to withhold the letter on the basis that its disclosure "could reasonably be expected to threaten the life or security of another individual". The following paragraph is the entire summary respecting the federal Privacy Commissioner's disposition of this significant issue:

> The Commissioner also had to determine if the company properly invoked section 9(3)(c). That is, could the information contained in the letter be reasonably expected to threaten the life or security of another individual? Upon review, the Commissioner was satisfied that the letter did not include words, statements or phrases that if released to the complainant, could reasonable be expected to threaten the life or security or another individual. The Commissioner determined that the company had also not properly invoked section 9(3)(c).

This summary illustrates, with respect, the difficulty one faces in seeking guidance from case summaries on issues that are potentially significant.

---

[20] PIPED Act Case Summary #103 (December 19, 2002).

In another case, the employer bank refused access to a file respecting an investigation the bank had conducted before dismissing the employee[21]. The bank had dismissed on of its branch managers for cause following the internal investigation. The bank disclosed the former employee's personnel file, but withheld the investigation file. The Privacy Commissioner first held that the bank had been authorized to collect personal information for the purposes of its investigation, which related to a possible breach of the former manager's employment agreement. He went on to determine that conclusion of the investigation did not preclude the bank from relying on s. 9(3)(c.1)). The protection afforded by that provision, in other words, is an ongoing one.

In another case, a former telecommunications company employee was denied access to information in his employment file. The company relied on s. 9(3)(d) to withhold some of the information, on the basis that it had been generated in the course of a formal dispute resolution process. The Privacy Commissioner apparently agreed that documentation relating to grievances relates to a formal dispute resolution process, thus allowing the company to rely on s. 9(3)(d). He also held, however, that some of the records were created as part of a "human rights investigation" and that such an investigation did not entitle the company to rely on s. 9(3)(d) in relation to those records. [22] The relevant case summary simply refers, without elaboration, to a "human rights investigation" of some kind and then asserts that the associated documentation was "not generated for the purposes of settling a dispute, but rather for the purpose of responding to allegations and providing a defence." It is difficult to discern from this a cryptic summary what kind of investigation was involved or what the reasoning was in arriving at the conclusion stated.

As regards the suggestion that a "human rights investigation" is not part of a formal dispute resolution process within the meaning of s. 9(3)(d) of PIPEDA, the federal Privacy Commissioner, in another case[23], said the following (quoting the case summary):

> With regard to section 9(3)(d), the Commissioner noted the purpose of this exception is not to protect information gathered in the course of administrative processes for resolving complaints or grievances. He further noted that such an interpretation would not respect principles of natural justice, effectively denying individuals their fundamental rights to know of allegations made against them and to know the basis of decisions made about them. Also in the Commissioner's view, a formal dispute-resolution process implies the desire of parties to meet for the purpose of *negotiating* a resolution acceptable to each – which was not the case with the parties in question. Hence he did not accept the employer's interpretation that the process was one of formal dispute-resolution or that the information at issue had been gathered strictly for that purpose. He determined that the employer had been wrong in applying section 9(3)(d) to refuse the complainant access to her personal information.

---

[21] PIPED Act Case Summary #84 (October 10, 2002).

[22] PIPED Act Case Summary #88 (October 31, 2002)

[23] PIPED Act Case Summary #37 (January 14, 2002)

It is not clear on what basis the federal Privacy Commissioner concluded that a process will be a formal dispute resolution process under s. 9(3)(d) only where the parties wish to negotiate an acceptable resolution. Nor is it clear what he meant by "fundamental rights to know of allegations made against them and to know the basis of decisions made about them" or how these "rights" drove his interpretation of this provision.

IV. Moving Forward

As indicated at the outset, the goals of this paper have been modest, as is necessitated by the absence of any tabled legislation in British Columbia, or even in Alberta, at the time of writing. It would be foolish to speculate on how British Columbia's private sector privacy law will shape up. It is safe to say, however, that PIPEDA necessarily will form the superstructure of that law. The need for substantial similarity in order for the federal government to bless the British Columbia law makes this plain. For the time being, this paper can do no more than offer some thoughts on selected employment issues that arise under PIPEDA. As for how British Columbia's law will affect employment relationship, stay tuned for a future CLE paper.

* * *